Google Scholar Crossref doi scopus

Impact factor 6.2

Geoscience Journal

ISSN:1000-8527

Indexing:

- Scopus
- Google Scholar
- DOI, Zenodo
- Open Access

www.geoscience.ac

Registered

Design and Development of IDS for wireless Network

1 Ms Archana P.Ambhore *Assistant Professor, Information Technology Department, Government College of Engineering, Amravati* , India
2. Premchand B.Ambhore, *Assistant Professor, Information Technology Department, Government College of Engineering, Amravati* Amravati, India

Abstract:. The notion of connecting objects to the Internet isn't novel. In the early 1990s, the first instances of controlling everyday items over the Internet emerged, laying the groundwork for today's IoT. Interactions with the Internet, whether personal, social, or economic, are undergoing a transformation. Currently, most users actively download and create content via computers and smartphones, but this trend is expected to change. Many IoT devices operate autonomously in the background, transmitting and receiving data with minimal human involvement. Some are designed to manage physical assets like vehicles and buildings, or to monitor human activities. As this shift occurs, it's essential to consider the potential impact of a world where passive interactions with connected devices become more common than active engagement with online content. Governments may need to adjust policies to address this changing dynamic. While the concept of IoT has existed for some time, its rapid growth presents both opportunities and challenges, requiring policy revisions. Privacy and data security policies will need to evolve to address the technological advancements and their effects on users. To support the development of IoT, efforts should focus on strengthening internet infrastructure, optimizing the use of wireless spectrum, expanding data centers, and empowering users. This will likely influence policies related to privacy, data security, healthcare, transportation, and technological innovation.

Keywords: Internet of Things (IoT), Machine Learning, Lightweight Cryptography, IDS.

1. INTRODUCTION

IoT has emerged fastest-growing technologies, significantly enhancing human convenience and comfort. By 2025, it is predicted that around 75 billion smart devices will be connected through IoT [1]. This technology plays a crucial role in various smart systems such as homes, transportation, agriculture, and industries, leading to improvements in efficiency, mobility, and cost reduction. However, IoT networks face higher security risks compared to other computing paradigms. To address the growing challenges in IoT networks, traditional security methods are proving insufficient. A more robust and comprehensive security approach is necessary to handle the demands of these networks. Existing security practices, including authentication, access control, and network protection, often fail to scale effectively for large IoT systems with numerous interconnected devices. The complexity of these networks— characterized by diverse technologies, distributed communication, and device heterogeneity creates significant vulnerabilities, exposing them to a wide range of cyber threats. Therefore, ensuring end-to-end security in IoT networks requires a robust and innovative solution. IoT networks consist of interconnected devices with unique identities. These devices gather data, which can either be processed locally or sent to a centralized cloud-based application for further analysis. After processing, the system can carry out tasks locally within the IoT infrastructure. IoT network data is nothing but raw and unprocessed obtain from IoT devices. Some applications like environment can consist of smart whether monitoring, smart air pollution monitoring, smart noise pollution monitoring and forest fire detection. Smart energy can consist of smart grid, smart renewable energy systems and smart prognostics. Smart retail can consist of smart inventory management smart payments and smart vehicle vending machines. Smart logistic can consist of smart road generation and scheduling smart remote vehicle diagnostics. Agriculture system can consist of smart irrigation and smart greenhouse control. Smart industry can consist of smart machine diagnosis and smart indoor quality monitoring. Smart health and lifestyle can consist of Health and fitness monitoring and wearable electronics. Applications of IoT can be benefited to the society for the wellbeing of society.

.

2 Literature Survey

In my research area, I have focused on security issue in IoT network, different aspects of this security issue are thoroughly studied in following literature.

2.1 IDS types suited for IoT networks 2.8.1 NIDS for IoT: This system monitors network traffic within IoT networks to detect suspicious activities and potential threats. It examines communication patterns among IoT devices, gateways, and backend systems to identify anomalies or recognized attack patterns. NIDS for IoT may utilize lightweight detection algorithms optimized for resource-constrained devices and low-power communication protocols typical in IoT setups. 2.8.2 Host-Based Intrusion Detection System (HIDS) for IoT Devices: HIDS deployed directly on IoT devices monitor local environments and device activities for signs of intrusion or compromise. They can detect unauthorized access attempts, unusual system behavior, or anomalous sensor readings indicative of a security breach. HIDS for IoT devices are engineered for efficient operation with minimal impact on device performance and energy consumption. 2.8.3 Behavioral Analysis and Anomaly Detection for IoT Networks: These techniques are invaluable for IoT networks, where normal operating conditions can vary widely based on application and environment. These IDS continuously learn and adapt to changes in IoT device behavior, enabling them to detect previously unseen threats and abnormalities suggestive of malicious activity or system compromise. 2.8.4 ML-Based IDS for IoT Networks: ML algorithms are trained to identify patterns and anomalies in IoT network traffic, empowering IDS to recognize sophisticated and evolving threats. ML-based IDS for IoT networks analyze large volumes of data from diverse sources, including sensor data, device telemetry, and network traffic, for real-time anomaly detection.

2.2 Distributed IDS Architecture for IoT Networks: Due to the distributed nature of IoT deployments, IDS for IoT networks may adopt a distributed architecture with multiple detection points dispersed across the network. This approach enables decentralized threat detection and response, reducing latency, and enhancing scalability in large-scale IoT deployments. 2.8.6 Protocol-Specific IDS for IoT Networks: Some intrusion detection systems (IDS) designed for IoT networks focus on analyzing specific communication protocols frequently used in these environments. These protocol-specific IDS can identify anomalies at the protocol level, unauthorized use of protocols, or attack patterns unique to each protocol, offering targeted security for IoT communication channels. These IDS are crucial for protecting IoT devices, data, and infrastructure from cyber threats and vulnerabilities. They use specialized detection techniques and algorithms to effectively identify and mitigate threats in the evolving IoT security landscape. According to the literature, machine learning approaches are also valuable for detecting and mitigating attacks in IoT networks, helping to address various vulnerabilities.

2.3 Overview of Lightweight Cryptography for End to End Secure Communication Cryptography. It is a fundamental component of modern information security, playing a critical role in safeguarding sensitive information, ensuring privacy, and upholding trust in digital communication and transactions. It is the method by which data can be encrypted for safe transmission. Also it can prevent altering of data. Cryptography is of two types Symmetric or Asymmetric [19].

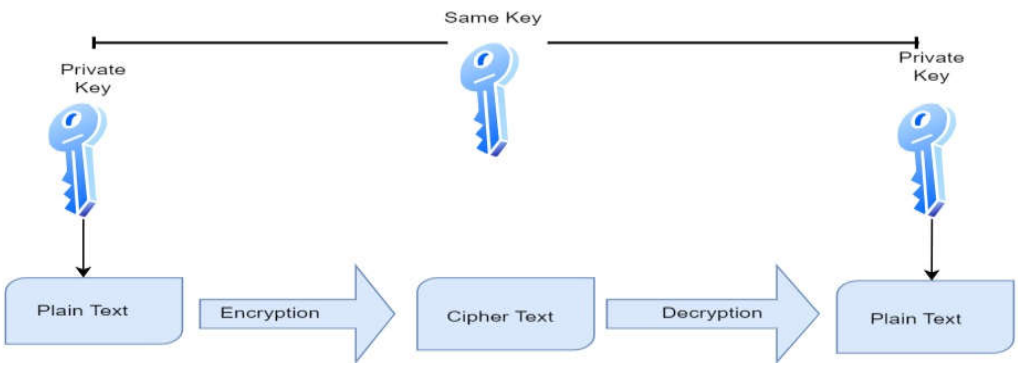

Figure 2.1: Symmetric Cryptography

Symmetric Cryptography: Figure 2.5 shows, it is a cipher technology which uses same Key for encryption and decryption. It is secure but when at the time of data transmission Key is falls in wrong hand the encrypted data is compromised [40]. Symmetric cryptography is of three cipher which are stream cipher, block cipher or hash function.

Asymmetric Cryptography: Figure 2.6 shows, it is a used in secure communication of data where two different keys are used for data confidentiality and integrity. Hence confidentiality as well as integrity is maintained as private key is known to only authenticated receivers. Sharing of key and high key size is the issue. It requires secure way for sharing[19].

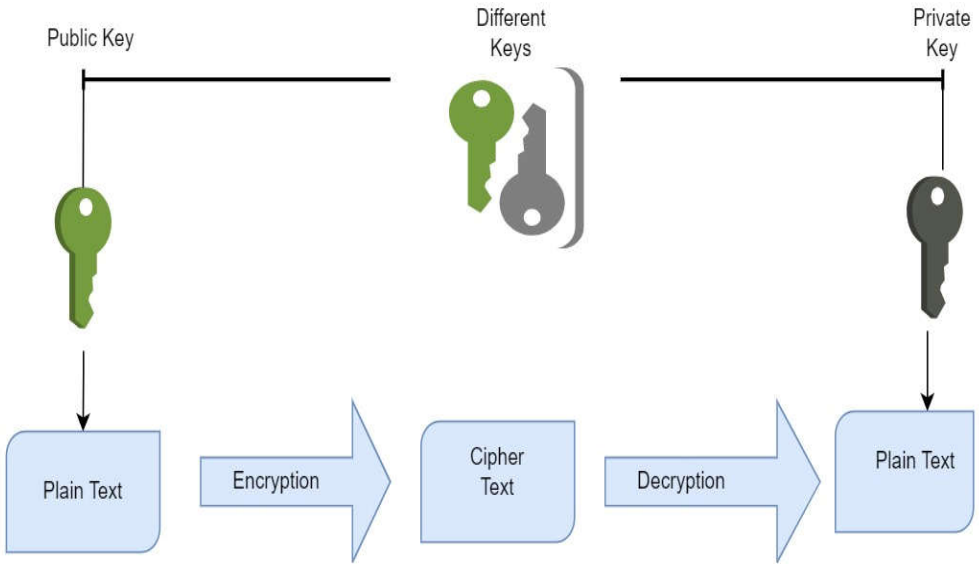

Figure 2.2: Asymmetric Cryptography

Due to various attacks observed at data in transit on IoT network its very essential to have any robust method to safeguard sensitive data of IoT devices. Sensitive information can be secured at the time of transit only with the help of cryptography. But traditional cryptographic algorithms cannot work for devices having low configuration. In IoT devices has low hardware configuration required lightweight solution of cryptography. Hence evolution of lightweight cryptography is done. 2.13 Lightweight Cryptography IoT devices face challenges when applying cryptographic techniques to secure them due to their limited resources such as small memory, computing power, and physical size, as well as the need for real-time responses. Designing cryptographic algorithms to protect data in these devices requires addressing these constraints [21] [22]. While cryptographic methods are commonly used for data security, some are not suitable for IoT devices due to their limited resources. This is where lightweight cryptography comes into play, offering encryption techniques tailored for pervasive devices with low resource requirements. The cryptographic algorithms chosen for securing IoT data must meet rigorous security standards, ensuring confidentiality, integrity, authentication, and non-repudiation . Additionally, algorithm design must consider both hardware and software capabilities. In terms of software, temporal complexity and memory usage, including RAM and ROM requirements, are crucial considerations. Hardware specifications categorize algorithms based on power consumption and latency, with low power consumption and minimal latency being essential for IoT device applicability

3. Methodology

3.1 IoT Simulators: Developing IoT projects often requires extensive hardware, including sensors and actuators. However, deploying a complete IoT network for every new idea or test is not always practical. This is where simulators become essential. They allow for the design of architectures, creation of prototypes, and testing of different attack models and threats. Depending on the requirements of a specific project, various IoT simulators can be used to facilitate these processes. Simulators Simulators are crucial tools for IoT (Internet of Things) research as they allow researchers to model and test various aspects. Here are some popular simulators used for IoT research: NS-3: NS-3 is open-source simulator for networking

research, and it can be extended to simulate IoT scenarios. It provides a comprehensive set of models for wireless communication, protocols, and networking. It has some Features like • High-level scripting and programming support. • Active community and continuous development. INET Framework for OMNeT++: The INET Framework is an extension for OMNeT++ that focuses on the simulation of internet protocols and applications. It can be used to simulate IoT scenarios with a focus on network-level aspects. It has some Features like • Extensive library of models for internet protocols. • Scalable and customizable for various simulation scenarios. • Support for wireless and wired networksFogNetSim++: FogNetSim++ is a simulator designed for fog and edge computing research. It allows researchers to model and simulate the interactions between cloud, fog, and IoT devices in a comprehensive manner. It has some Features like • Support for fog and edge computing scenarios. • Integration with cloud platforms. • Simulation of resource allocation and data processing. ThingSim: ThingSim is a simulator designed for simulating IoT devices and networks. It is particularly focused on energy-efficient communication and networking protocols for IoT. It has some Features like • Simulation of energy-efficient communication. • Customizable for various IoT scenarios. • User-friendly graphical interface. NetSim Standard: NetSim is a simulator for designing IoT networks. In Netsim standard code updation can be possible hence used for Research and Development. It has some Features like • Develop and simulate own protocols and algorithms. • Inbuilt interface with MATLAB and Wireshark etc. • It has protocol source C code. In this work, design of IoT network is done using NetSim simulator.

3.2 Machine Learning approaches: Techniques of Machine Learning are helpful for identification of network attacks. Machine learning is nothing but series of algorithms. These algorithms can learn patterns from available data and do predictions. Hence this approach is used for identification of attacks also possible to avoid it. The most commonly used Machine Learning techniques using Supervised Machine Learning approaches are Decision Trees, Bayesian algorithm, K-nearest neighbor (KNN), Support Vector Machine (SVM), Random Forest (RF) and Association Rule (AR). Also most commonly used Unsupervised Machine Learning approaches are K-Means Clustering (KMC)and Principal Component Analysis. Depending on need of application any one approach can be used.

Algorithm: Anomaly Detection Using Machine Learning Approach

INPUTS: Datasets, machine learning models

OUTPUT: Anomaly Detector

PROCEDURE:

Step - 1: Read Live traffic of IoT network.

Step - 2: Apply machine learning model

Step - 3: Train the machine learning model to detect normal/abnormal traffic trend

Step - 4: Test the traffic

Step - 5: **if** traffic trend is abnormal then

Step - 6: Block traffic

Step - 7: else

Step - 8: Allow traffic

Step - 9: end if

Design of Cloud based IoT Network Scenario using license software NetSim Standard v13.3

Step 1. Creating a Cloud based IoT Network Scenario using sensor nodes, 6LoWPAN gateway, routers and Cloud Server Configuring Devices and Links can be possible by setting properties to devices as well as links. Modeling Application Traffic is done by establishing application

between Sensor node 1 and Cloud Server. In this IoT Network Scenario Wireless Sensor Node 6 and Wireless Sensor Node 8 are declared as Malicious node with the help of code.

Step2. Run Simulation for capturing live traffic between sensor nodes like Wireless _Sensor_1 upto Wireless_Sensor_16 of Cloud based IoT network and also between Application_1 which is for capturing live traffic from Wireless_Sensor_1 to Wired_Node 20.

Step 3. Enabling Plots and Traces can be made enabled for generating it after completion of simulation. Following metrics are generated after simulation is completed which consists of Application_Matrics_Table, TCP_Metrics_Table, Link_Metrics_Table, Queue_Mterics_Table In Application Metrics for App1_SENSOR_App Packet Generated 100 but Packet Received is 0. Hence Throughput is 0.000000. All packets of App1_SENSOR_App are dropped by malicious Node 6 and Node 8.

Step 4. Packet Trace option is available for generating log of Sensor data.Captured Live Sensor data is now can be analysed for attack detection and The data transmitted of App1_Sensor _App from Sensor Node 1 is reached to Sensor Node 6 and Sensor Node 8 and dropped as these are malicious nodes

4 Analysis

4.1 Detection of the Sinkhole Node: In this a node which is malicious will falsely advertises a beneficial route, attracting nearby nodes to direct their traffic through it. While this attack doesn't immediately disrupt the network, it becomes highly dangerous when combined with other types of attacks. This section introduces an efficient security method based on the RPL protocol. • A node that provides its true rank to neighbors is unlikely to be malicious. • A node sending multiple DIO messages to non-child neighbors could be suspicious. • A node that misrepresents its rank is considered malicious. To prevent routing loops, the RPL protocol calculates the hop count known as DODAG. In this context, it is used to represent the node's position. The rank provides valuable information for estimating distance from the root node, and the proposed system leverages this rank value to detect suspicious values in DIO messages. The RPL protocol includes an ICMPv6 control message for exchanging routing graph information. An attacker may attempt to exploit this by sending fake ICMPv6 routing packets to create a sinkhole.

Fake Rank Detection in RPL Log: Following figure 5.9 shows Node 6 and Node 8 declares fake rank.

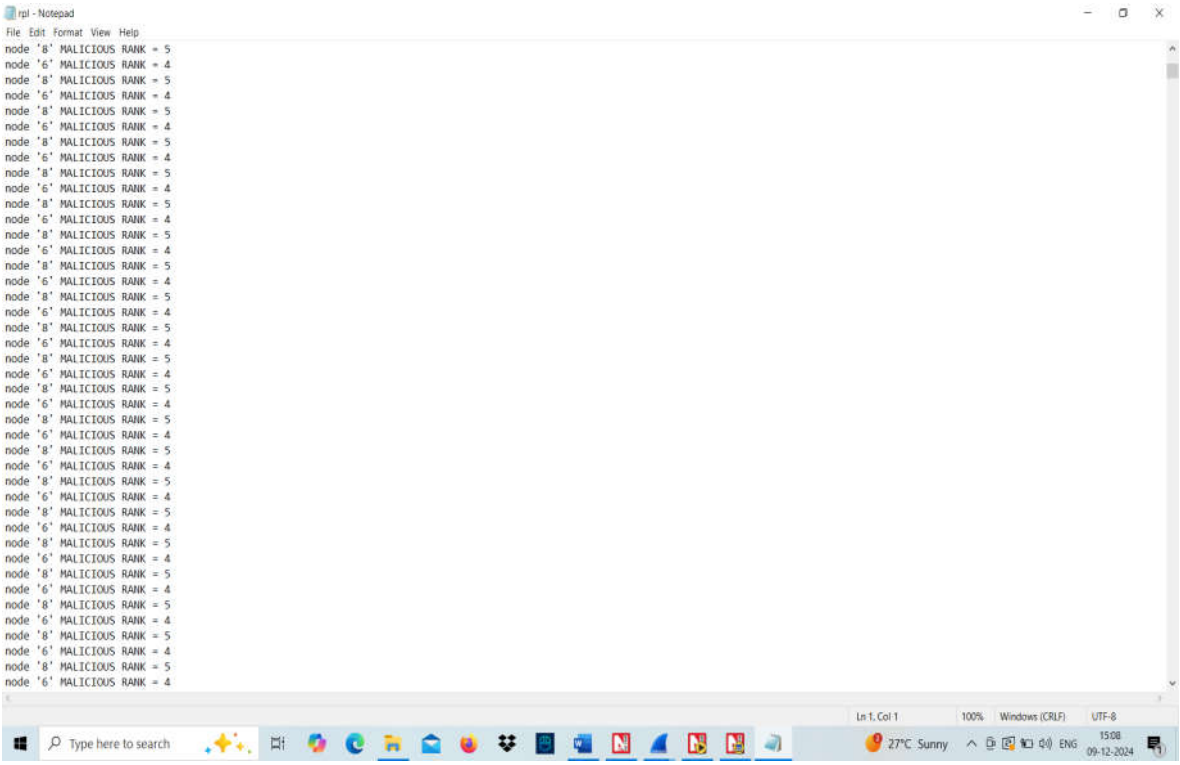

Figure: 4.1 Fake Rank Detection in RPL Log

5. Implementation of Attack Detection and Mitigation

Step1: Once a a packet is forwarded in a IoT network, it will reach to next node within some specific time. Current node check for duration or time required to reach to next node if the timer is expiring count is increased by one for counter. If this counter value cross threshold value the next node will be marked as malicious node. Timer and Counter are set in coding for IoT network attack detection and mitigation. When these malicious nodes are detected in IoT network, route is changed for packet by route discovery process and packets reached to destination, which is done with the help of coding. Following Figure 5.11 shots shows how IDS_Metrics_Table demonstrated Node 6 and Node 8 are malicious with Start time (Node behaves like malicious from that time) and detection time (Node actually added to blacklist on that time). Application Metrics shows Packet Generated 500 and Received Packets are 0. Hence Throughput is 0.000000. All Packets are reverted back to Node 1. In this delay of 1500000.0 microsecond is set to Node 6 and delay of 15.000000 microseconds is set to Node 8 for attack detection. Hence some Anamoly can be captured and this will be useful for creation of Data Set.

Packet Trace option is available for generating log of Sensor data.Captured Live Sensor data is now can be analysed for attack detection and mitigation as shown in Figure 5.1. In this file in Transmission ID Column we can observe packets transmitted from malicious node Sensor Node 6 and Sensor Node 8 are not forwarded in IoT network rather revert back to Node1. Hence these data packets are declared as Anomaly and rest packets are Normal in the Dataset.

Step 3: Preprocessing on Sensors Live Captured data file for Creation of IoT Dataset: Preprocessing is done on Live Captured IoT Sensors data and Last Column ‘Label’ is added In .csv file as Anomaly for Packets transmitted from Node 6 and Node 8 because these are malicious nodes remaining packets are Normal as shown in figure 5.2

5.1 End to end Secure Communication of Cloud Based IoT Network It is necessary to upload IoT sensors data on Cloud for Secure communication of cloud based IoT network. Implementation Screen Shots for creating AWS S3 storage and Uploading .CSV file of IoT Sensor data on Cloud 5.1 Login to AWS Management Console First step is to create AWS Management Console and login to this console as shown in Figure 5.2

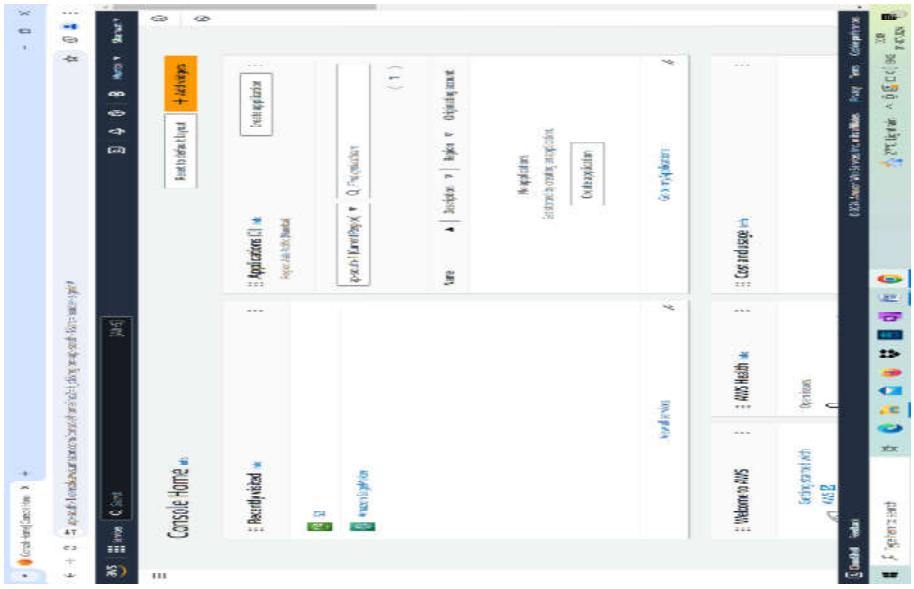

Figure: 5.1 Screen Shot of Login AWS Management Console

5.2 Amazon S3 Service Search for S3 Service and Click on Create Bucket to get started as shown in Figure 5.29.

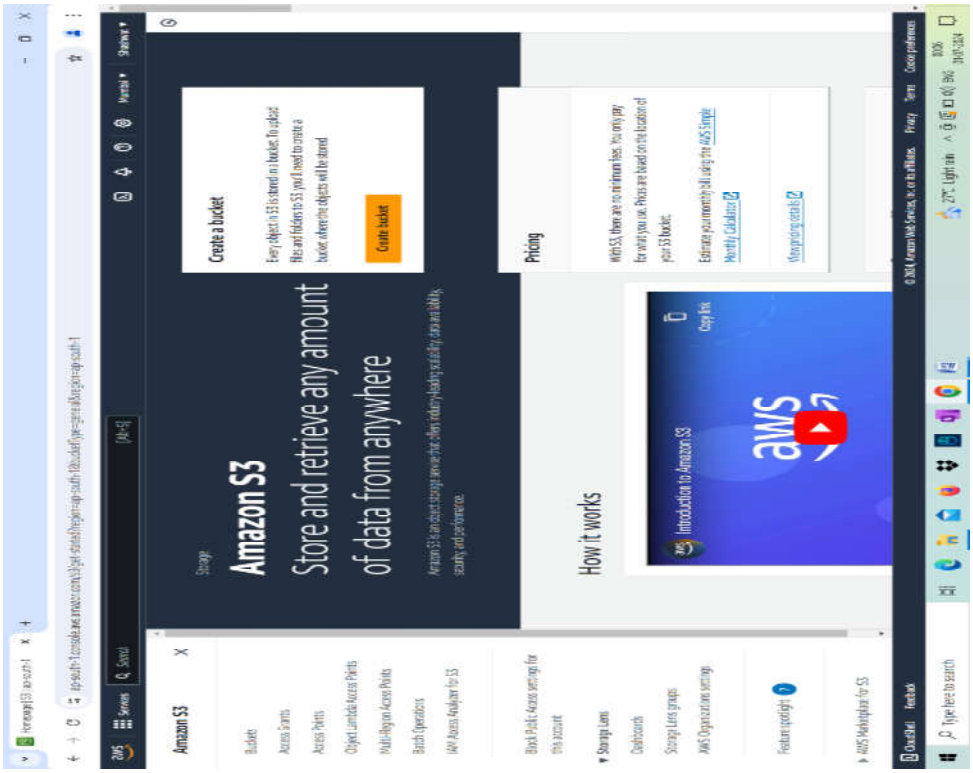

Figure: 5.2 Screen Shot of Amazon S3 Service

5.2 Bucket Creation Following Figure 5.4 Screen Shot shows successful creation of Bucket named “cloud communication” in Amazon S3

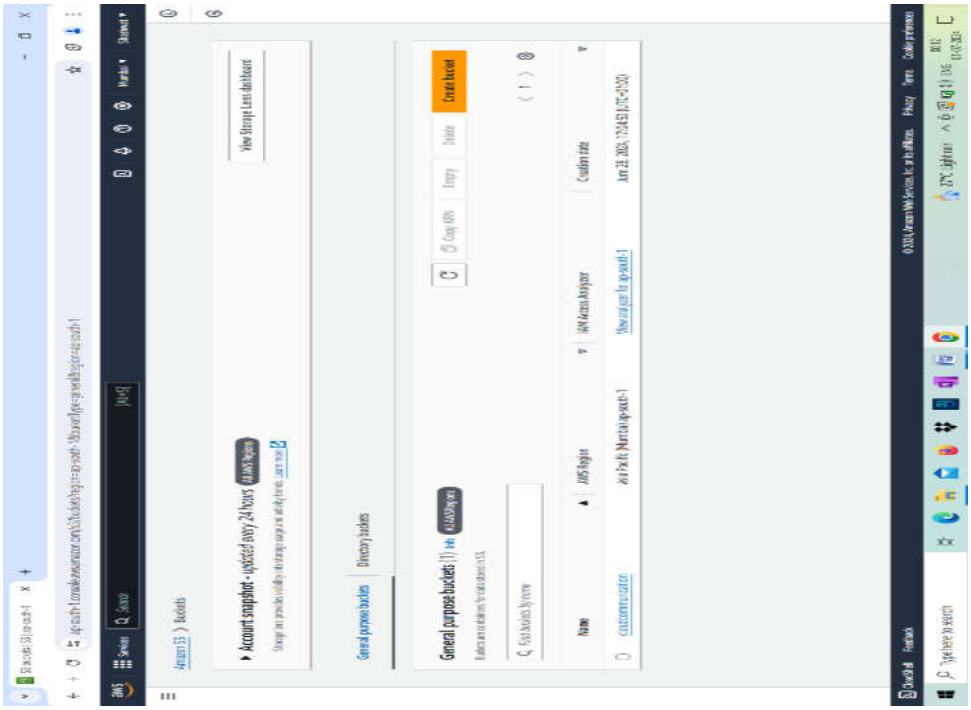

Figure: 5.3 Screen Shot of successful creation of Bucket in Amazon S3

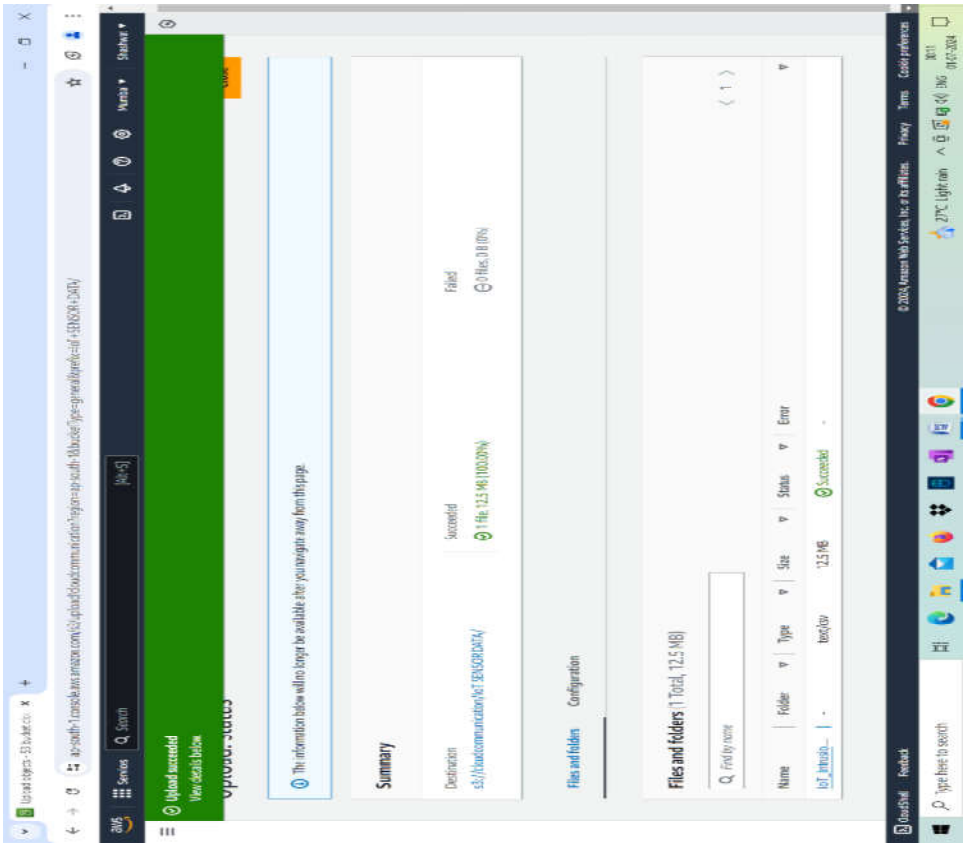

Figure: 5.4 Screen Shot of Successful Upload of .csv File

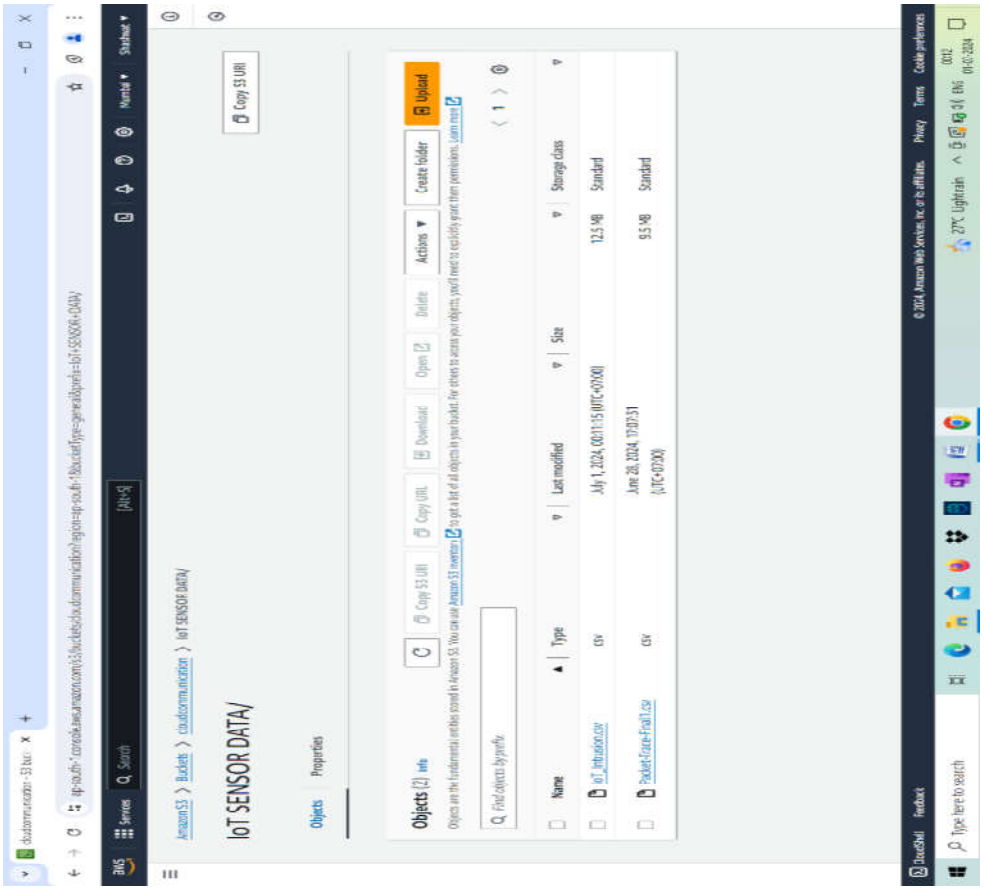

Figure: 5.5 Screen Shot of IoT Sensor data Uploaded

Conclusion

IoT presents distinct security challenges that demand collaborative efforts to develop solutions that align with the scale and complexity of the technology. Insufficient security in devices and services can leave user data vulnerable to cyberattacks, especially as the number of connected devices increases. Manufacturers encounter both technical and financial obstacles when trying to implement robust security measures, emphasizing the importance of long-term strategies to uphold user trust.

REFERENCE

[1] Abbas, Ghulam, AmjadMehmood, Maple Carsten, Gregory Epiphaniou, and Jaime Lloret. "Safety, Security and Privacy in Machine Learning Based Internet of Things" *Journal of Sensor and Actuator Networks* 11, no. 3: 38, 2022,doi.org/10.3390/jsan11030038.

[2] Kamaldeep, M. Dutta and J. Granjal, "Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms," in IEEE Access, vol. 8, pp. 127272-127312, 2020, doi: 10.1109/ACCESS.2020.3005643.

[3] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.

[4] M. Rana ,Q.Mamun, R. Islam "Lightweight cryptography in IoT networks: A survey", *Journal Future Generation Computer Systems*,Vol.129,pp.77-89,2022,doi.org/10.1016/j.future.2021.11.011

[5] H. Tawalbeh , S. Hashish ,"Security in Wireless Sensor Networks Using Lightweight Cryptography", in Journal of Information Assurance and Security, ISSN 1554-1010 ,Volume 12, pp. 118-123, 2017.

[6] C. Silva, V. A. Cunha, J. P. Barraca, R. L. Aguiar "Analysis of the Cryptographic Algorithms in IoT Communications",in Springer Information Systems Frontiers, doi: 10.1007/s10796-023-10383-9,2023.

[7] Fotovvat, G. M. E. Rahman, S. S. Vedaei and K. A. Wahid, "Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8279-8290, 15 May15, 2021, doi: 10.1109/JIOT.2020.3044526.

[8] VikasHassija ,VinayChamola, VikasSaxena, Divyansh Jain, PranavGoyal , and BiplabSikdar: A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,IEEE Access,Vol.7,(2019).
[9] Francesca Meneghello, MatteoCalore, Daniel Zucchetto , Michele Polese , and Andrea Zanella: IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices, IEEE Internet of Things Journal, Vol. 6, NO. 5, October (2019).
[10] Nadia Chaabouni, Mohamed Mosbah , AkkaZemmari, CyrilleSauvignac, and ParvezFaruki: Network Intrusion Detection for IoT Security Based on Learning Techniques, IEEE Communications Surveys& Tutorials, Vol. 21, No. 3, Third Quarter (2019).
[11] Fatima Hussain, ,RasheedHussain , Syed Ali Hassan , and EkramHossain : Machine Learning in IoT Security: Current Solutions and Future Challenges,IEEE Communications Surveys & Tutorials, Vol. 22, No. 3, Third Quarter (2020).
[12] Mohammed Ali Al-Garadi, Amr Mohamed ,Abdulla Khalid Al-Ali , Xiaojiang Du ,Ihsan Ali , and Mohsen Guizani : A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security, IEEE Communications Surveys & Tutorials ,Vol. 22, No. 3,Third Quarter (2020).
[13] Oracle Corporation, (n.d.), "What is IoT?", last accessed on 10 October 2023, https://www.oracle.com/internet-of-things/what-is-iot/
[14] Gyamfi, E.; Jurcut, A., "Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets", *Sensors 2022*, 22, 3744. https://doi.org/10.3390/s22103744
[15] Cisco Systems, Inc., March 10, 2020, "Cisco Annual Internet Report (2018–2023) White Paper", last accessed on 5 May 2023, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html
[16] Joyanes Aguilar, L.,"Hiperconectividad: Infraestructuras de Comunicaciones", "Infrastructures de la Internet de las Cosas: Cloud Computing, Edge, y Fog computing", "Seguridad y ciberseguridaden Internet de lasCosas", *Internet de lascosas, Un futurohiperconectado: 5G, Inteligencia Artificial, Big Data, Cloud, Blockchain, Ciberseguridad*, pp. 55-90, 141-178, 281-309, Marcombo, S.L., 2021
[17] Power Solution, (n.d.), "Fog Computing and Edge Computing: What You Need to Know", last accessed on 28 June 2023, https://www.power-solutions.com/industry-trends/fog-computing-and-edge-computing-what-you-need-to-know/
[18] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," Wireless Netw., vol. 20, no. 8, pp. 2481–2501, 2014.
[19] J. Chen, S. Kher, and A. Somani, "Distributed fault detection of wireless sensor networks," in Proc. Workshop Dependability Issues Wireless Ad Hoc Netw.SensorNetw. (DIWANS), 2006, pp. 65–72.
[20] Himanshu V. Taiwade, Premchand B.Ambhore "Hybrid bioinspired approach for secret sharing algorithm and ownership transfer optimization in cloud-based models" Journal of Discrete Mathematical Sciences and Cryptography, January 2024;625-637
[21] Dutta, N.S., and Chakraborty, S. A survey on implementation of lightweight block ciphers for resource constraints devices. Journal of Discrete Mathematical Sciences and Cryptography.2020; 1–22.
[22] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," in IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 903-912, Feb. 2021, doi: 10.1109/TII.2020.2968927
[23] C. Liu, Y. Zhang, J. Xu, J. Zhao and S. Xiang, "Ensuring the Security and Performance of IoT Communication by Improving Encryption and Decryption With the Lightweight Cipher uBlock," in IEEE Systems Journal, vol. 16, no. 4, pp. 5489-5500, Dec. 2022, doi: 10.1109/JSYST.2022.3140850.
[24] A. Jamalipour and S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9444-9466, 15 June15, 2022, doi: 10.1109/JIOT.2021.3126811
[25] A. K. Pathak, S. Saguna, K. Mitra and C. Åhlund, "Anomaly Detection using Machine Learning to Discover Sensor Tampering in IoT Systems," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500825
[26] G. Said, A. Ghani, A. Ullah, M. Azeem, M. Bilal and K. S. Kwak, "Light Weight Secure Aggregated Data Sharing in IoT-Enabled Wireless Sensor Networks," in IEEE Access, vol. 10, pp. 33571-33585, 2022, doi: 10.1109/ACCESS.2022.3160231
[27] R. Sivakumar, J. Jayapriya and N. Krishnan, "Comparison Study on SPN Type Light Weight Cryptography Algorithms for IoT," 2022 International Conference on Inventive Computation Technologies (ICICT), Nepal, 2022, pp. 1051-1055, doi: 10.1109/ICICT54344.2022.9850849
[28] A. I. Regla and E. D. Festijo, "Performance Analysis of Light-weight Cryptographic Algorithms for Internet of Things (IoT) Applications: A Systematic Review," 2022 IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 2022, pp. 1-5, doi: 10.1109/I2CT54291.2022.9824108

[29] MuhammadRana,QuaziMamun,RafiqulIslam"Lightweight cryptography in IoT networks: A survey", Journal Future Generation Computer Systems,Vol.129,pp.77-89,2022,doi.org/10.1016/j.future.2021.11.011
[30] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, “Machine learningin wireless sensor networks: Algorithms, strategies, and applications,”IEEE Commun. Surveys Tuts., vol. 16, no. 4, pp. 1996–2018,Oct.–Dec. 2014
[31] Hsing-Chung Chen and Ilsun You and Chien-ErhWeng and Chia-Hsin Cheng and Yung-Fa Huang,"A security gateway application for End-to End M2M communications", Computer Standards & Interfaces,Vol.44,pp.8593,2016,doi.org/10.1016/j.csi.2015.09.001.
[32] Xuezhi Zeng and Saurabh Kumar Garg and Peter Strazdins and Prem Prakash Jayaraman and DimitriosGeorgakopoulos and Rajiv Ranjan,"IOTSim: A simulator for analysing IoT applications", Journal of Systems Architecture,Vol.72,pp.93-107,2017,doi.org/10.1016/j.sysarc.2016.06.008
[33] M. S. A. Muthanna, R. Alkanhel, A. Muthanna, A. Rafiq and W. A. M. Abdullah, "Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT)," in IEEE Access, vol. 10, pp. 22756-22768, 2022, doi: 10.1109/ACCESS.2022.3153716.
[34] M. Chernyshev, Z. Baig, O. Bello and S. Zeadally, "Internet of Things (IoT): Research, Simulators, and Testbeds," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1637-1647, June 2018, doi: 10.1109/JIOT.2017.2786639
[35] M. Khoda, T. Imam, J. Kamruzzaman, I. Gondal and A. Rahman, "Robust Malware Defense in Industrial IoT Applications Using Machine Learning With Selective Adversarial Samples," in IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4415-4424, July-Aug. 2020, doi: 10.1109/TIA.2019.2958530.
[36] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," in IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 903-912, Feb. 2021, doi: 10.1109/TII.2020.2968927.
[37] N. Ravi and S. M. Shalinie, "Semisupervised-Learning-Based Security to Detect and Mitigate Intrusions in IoT Network," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 11041-11052, Nov. 2020, doi: 10.1109/JIOT.2020.2993410.
[38] C. Liu, Y. Zhang, J. Xu, J. Zhao and S. Xiang, "Ensuring the Security and Performance of IoT Communication by Improving Encryption and Decryption With the Lightweight Cipher uBlock," in IEEE Systems Journal, vol. 16, no. 4, pp. 5489-5500, Dec. 2022, doi: 10.1109/JSYST.2022.3140850.
[39] A. K. Pathak, S. Saguna, K. Mitra and C. Åhlund, "Anomaly Detection using Machine Learning to Discover Sensor Tampering in IoT Systems," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500825.